UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/974,705	10/10/2001	Marco Macchetti	01AG17653537	7872

27975 7590 02/08/2010

ALLEN, DYER, DOPPELT, MILBRATH & GILCHRIST P.A.
1401 CITRUS CENTER 255 SOUTH ORANGE AVENUE
P.O. BOX 3791
ORLANDO, FL 32802-3791

EXAMINER	
COLIN, CARL G	

ART UNIT	PAPER NUMBER
2433	

NOTIFICATION DATE	DELIVERY MODE
02/08/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

creganoa@addmg.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte MARCO MACCHETTI, STEFANO MARCHESIN,
UMBERTO BONDI, LUCA BREVEGLIERI, GUIDO BERTONI,
and PASQUALINA FRAGNETO

Appeal 2008-005061
Application 09/974,705
Technology Center 2400

Decided: February 4, 2010

Before LANCE LEONARD BARRY, JOHN A. JEFFERY, and
JAMES R. HUGHES, *Administrative Patent Judges*.

JEFFERY, *Administrative Patent Judge*.

DECISION ON APPEAL

Appellants appeal under 35 U.S.C. § 134(a) from the Examiner's rejection of claims 21-25, 27-43, and 48-51. Clams 1-20, 26, and 44-47 have been canceled. *See* Supp. Br. 2. We have jurisdiction under 35 U.S.C. § 6(b). We affirm.

STATEMENT OF THE CASE

Appellants invented a method and device that encrypts data through several transformation rounds. The method uses a state array or matrix to transform the data and includes a step of exchanging each row of the state array for the columns of the state array during at least one of the transformation rounds. This arrangement simplifies the system and increases the system's speed.[1]

Independent claim 21 is reproduced below with the key disputed limitations emphasized:

> A method of converting data between an unencrypted format and an encrypted format, the data being organized in bit words, the method comprising:
>
> converting the data by at least performing a plurality of transformation rounds comprising
>
> applying at least one transformation to a two-dimensional array of rows and columns of bit words defining a state array;
>
> *exchanging each of the rows with a respective column of the state array to form a transposed state array for at least one of the transformation rounds so that the at least one transformation is applied to the transposed state array*; and
>
> applying at least one round key to the state array in at least one of the transformation rounds.

The Examiner relies on the following as evidence of unpatentability:

Luther	US 5,533,127	July 2, 1996
Ohkuma	US 2001/0024502 A1	Sept. 27, 2001

[1] *See generally* Spec 8-10; Figs. 5-6.

THE REJECTION

The Examiner rejected claims 21-25, 27-43, and 48-51 under 35 U.S.C. § 103(a) as unpatentable over Ohkuma and Luther. Ans. 3-11.[2]

CLAIM GROUPING

Appellants argue independent claims 21, 31, and 48 as a group. *See* Br. 5-10. Appellants do not separately argue dependent claims 22-25, 27-30, 32-43, and 49-51. *See id*. Accordingly, we select claim 21 as representative. *See* 37 C.F.R. § 41.37(c)(1)(vii).

CONTENTIONS

Regarding representative claim 21, the Examiner finds that Ohkuma explicitly discloses all the limitations, except for exchanging each of the rows with a respective column of the state array to form a transposed state array. Ans. 3-4. The Examiner cites Luther to cure this deficiency, and contends that a skilled artisan would have modified Ohkuma to exchange each row with respective columns of a state array to confuse the data further. Ans. 4.

Appellants argue that Luther fails to exchange rows with a respective column of the state array to form a transposed state as claimed. Br. 5-10. Appellants contend that the invert-bit function in Luther complements the

[2] Throughout this opinion, we refer to (1) the Appeal Brief filed September 7, 2007 and supplemented October 11, 2007, and (2) the Examiner's Answer mailed November 28, 2007.

rows and columns rather than transposes them. Br. 8-9. Additionally, Appellants contend that Luther does not complement each row and column, but skips rows and columns. Br. 9.

The issue before us, then, is as follows:

ISSUE

Under § 103, have Appellants shown that the Examiner erred in rejecting claim 21 by concluding that Ohkuma and Luther collectively teach or suggest "exchanging each of the rows with a respective column of the state array to form a transposed state array?"

FINDINGS OF FACT

The record supports the following findings of fact (FF) by a preponderance of the evidence:

Ohkuma

1. Ohkuma discloses encrypting a data set in the form of a matrix from one set of values to another set of values. ¶¶ 0062-65; Fig. 1.

2. This technique involves rounds of transformation using transformation modules 2 and diffusion modules 3. The diffusion modules 3 include a Maximum Distance Separable (MDS) matrix or high-level MDS matrix (e.g., MDS_H shown in Fig. 1). ¶ 0062 and 0076; Fig. 1.

3. Ohkuma discloses an example of a high-level MDS matrix used in encryption and a circuit used to transform data. ¶¶ 0261-63, 0273-74; Figs. 30 and 32.

4. Ohkuma discloses that "a matrix obtained by substituting rows, substituting columns, and arbitrarily transposing in an arbitrary MDS matrix may be used." ¶ 0268.

Luther

5. Luther teaches an encryption system that involves a substitution of a swap row/column end around function of an M row by N column two-dimensional matrix of a data signal. Col. 1, ll. 35-39, col. 4, ll. 42-45, and col. 6, ll. 12-16; Figs. 6 and 8.

6. Luther teaches the swap row/column end around function is implemented when executing steps S211 and S215 in order to confuse the data further. Col. 6, ll. 12-16.

7. Luther teaches one example of encrypting the data signal matrix's rows by selecting a value for S or "stripe height." If S equals one, the third, fourth, sixth, seventh, ninth, tenth, twelfth, and thirteenth rows are encrypted. If S is selected to be two (i.e., S=2), the third through the fourteenth rows are encrypted. Col. 4, ll. 42-54.

8. Luther teaches encrypting the data signal matrix's columns by selecting a value for S or "strip height." If S equals one, the fourth, fifth, eighth, ninth, twelfth, and thirteenth columns are encrypted.[3] If S is selected to be 2 (i.e., S=2), the fourth, fifth, sixth, eighth, ninth, tenth, twelfth, thirteenth, and fourteenth columns are encrypted. Col. 4, l. 58 – col. 5, l. 3.

[3] Luther states "rows" but we presume this was a typographical error because the entire paragraph discusses encrypted columns of a data signal matrix. *See* col. 4, l. 58 through col. 5, l. 3.

PRINCIPLES OF LAW

In rejecting claims under 35 U.S.C. § 103, it is incumbent upon the Examiner to establish a factual basis to support the legal conclusion of obviousness. *See In re Fine*, 837 F.2d 1071, 1073 (Fed. Cir. 1988). If the Examiner's burden is met, the burden then shifts to the Appellants to overcome the prima facie case with argument and/or evidence. Obviousness is then determined on the basis of the evidence as a whole and the relative persuasiveness of the arguments. *See In re Oetiker*, 977 F.2d 1443, 1445 (Fed. Cir. 1992).

ANALYSIS

Based on the record before us, we find no error in the Examiner's obviousness rejection of representative claim 21 which calls for, in pertinent part, exchanging each of the rows of a state array with a respective column of the state array to form a transposed state array. Ohkuma discloses an encryption technique that converts a data set described as a matrix from one set of values to another set of values. FF 1. This technique involves several transformation rounds using transformation modules 2 and diffusion modules 3. FF 2. The diffusion modules 3 include a Maximum Distance Separable (MDS) matrix or high-level MDS matrix (e.g., MDS_H shown in Fig. 1). *Id.* One such example of a high-level MDS matrix used in encryption is shown in Figure 30 and transforms the data using the circuit shown in Figure 32. FF 3. Ohkuma further discloses obtaining such a matrix "by substituting rows, substituting columns, and arbitrarily *transposing* in an arbitrary MDS matrix . . . ." FF 4 (emphasis added).

At a minimum, this portion of Ohkuma (*id.*) suggests using a transposed matrix while converting data from an unencrypted format to an encrypted format during transformation. *See* FF 1-4. Moreover, since transposing a matrix involves exchanging its rows with respective columns,[4] Ohkuma's teaching of an arbitrarily transposing a matrix would do no more than yield a predictable result of producing encrypted data by exchanging each of the rows with a respective column of the state array to form a transposed state array as recited in claim 21. *See KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 416 (2007).

Additionally, Luther teaches an encryption technique that involves a substitution of a swap row/column end around function of an M row by N column two-dimensional matrix of a data signal. FF 5. In particular, Luther teaches this swap row/column end around function is implemented during the execution of steps S211 and S215 in order to confuse the data further. FF 6. As explained above, swapping or exchanging rows and columns of a matrix is a transposition and, thus, this portion of Luther suggests exchanging each of the rows with a respective column of an array as recited in claim 21 to confuse the data further.

Appellants argue that this section of Luther teaches complementation and not transposition. Br. 8-9. We disagree. First, Luther states that the encryption process involves a function that swaps the rows and columns (i.e., transposes) the matrix of a data signal. Second, this portion discusses an additional function (i.e., substitution of a swap row/column end around function) can occur when executing steps S211 and S215 or during

[4] "Transposition means exchange of rows and columns of a matrix." Riaz A. Usmani, *Applied Linear Algebra* 34 (1987).

complementing the data signals. *See* FF 6. Luther therefore teaches not only complementing data signals, but also transposing a data signal matrix to confuse the data further during encryption.

Appellants also contend that the Luther skips a number of rows and columns during complementation based on random variables and, therefore, the iterations do not match up for transposing each row and column of the array. Br. 9. Luther teaches one example of encrypting a data signal that involves selecting S or "stripe height" to be one. FF 7. In this scenario, Appellants are correct that not all rows are encrypted, but only the third, fourth, sixth, seventh, ninth, tenth, twelfth, and thirteenth rows are encrypted. FF 7. But if S is selected to be two, more rows are encrypted. *Id.* That is, by selecting S to be two, more columns of the data signal matrix are encrypted than if S is one. FF 8. Ordinarily skilled artisans would have readily understood from this teaching that selecting higher values of S will encrypt more rows, and would predictably result in a value of S that will encrypt all rows and columns of the data signal matrix such that no rows or columns are skipped. Moreover, this teaching provides artisans with a finite number of predictable solutions and ample reason to pursue these options within their grasp. *See KSR*, 550 U.S. at 421. We therefore disagree with Appellants (App. Br. 9) that the row and column iterations cannot match up for transposition.

For the foregoing reasons, we find that the Examiner has not erred in concluding that Ohkuma and Luther collectively teach or suggest exchanging each row with a respective column of the state array to form a

transposed state array as recited in claim 21. We therefore sustain the Examiner's rejection of claim 21, and claims 22-25, 27-43, and 48-51 which fall with claim 21.

CONCLUSION

Appellants have not shown that the Examiner erred in rejecting claims 21-25, 27-43, and 48-51 under § 103.

ORDER

The Examiner's decision rejecting claims 21-25, 27-43, and 48-51 is affirmed.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a)(1)(iv).

AFFIRMED

pgc

ALLEN, DYER, DOPPELT, MILBRATH & GILCHRIST P.A.
1401 CITRUS CENTER 255 SOUTH ORANGE AVENUE
P.O. BOX 3791
ORLANDO FL 32802-3791

EVIDENCE APPENDIX

Riaz A. Usmani, *Applied Linear Algebra* 34-36 (1987).

Auto-Fill | Add A Page | Delete Last Page

Notice of References Cited	Application/Control No. 09/974,705	Applicant(s)/Patent Under Reexamination	
	Examiner Carl Colin	Art Unit 2400	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
	A	US-			
	B	US-			
	C	US-			
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	Riaz A. Usmani, "Applied Lineaar Algebra" (1987) pp. 34-36
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Welcome to the United States Patent And Trademark eContent Collection

eBook Details

Applied Linear Algebra
Monographs and Textbooks in Pure and Applied Mathematics ; 105

by Noble, Ben A.

View this eBook

Add to Favorites
Email this Information

Publication: New York Marcel Dekker, Inc., 1987.
Subject:
Algebras, Linear.
Language: English

Find Resources

Viewing Requirements
Ebrary Reader Plug-in is required.

Select your Interface Language:

English | 中文 (繁體) (Chinese) | 한국어 (Korean)
Español (Spanish) | 中文 (简体) (Chinese) | Italiano (Italian)
Français (French) | 日本語 (Japanese) | Dutch (Dutch)
Deutsch (German)

8. Show that $(A + B)^2 = A^2 + 2AB + B^2$ if and only if the square matrices A and B commute.

9. Prove that the set V of all 2×2 matrices A with real coefficients such that $AB = BA$ is a vector space under the operations of matrix addition and scalar multiplication, where

$$B = \begin{bmatrix} 1 & 2 \\ 3 & 1 \end{bmatrix}$$

Show that V has dimension 2 by verifying that the set of matrices $\{I, B\}$ forms a basis for V.

10. Let A, B, and C be nonzero matrices with $AB = C$. Prove that the columns of C are linearly dependent on the columns of the matrix A. Similarly, prove that the rows of the matrix C are linearly dependent on the rows of the matrix B.

11. Let

$$A = \begin{bmatrix} 3 & 2 & 2 \\ 1 & 4 & 1 \\ -2 & -4 & -1 \end{bmatrix}$$

Show that $|A - xI| = f(x) = (-1)^3[x^3 - 6x^2 + 11x - 6]$. Evaluate the matrix polynomial $f(A)$.

12. Show that

$$\begin{bmatrix} 1 & 0_{1,n-1} \\ 0_{n-1,1} & A_{n-1,n-1} \end{bmatrix} \begin{bmatrix} a & 0_{1,n-1} \\ 0_{n-1,1} & B_{n-1,n-1} \end{bmatrix} \begin{bmatrix} 1 & 0_{1,n-1} \\ 0_{n-1,1} & C_{n-1,n-1} \end{bmatrix} = \begin{bmatrix} a & 0_{1,n-1} \\ 0_{n-1,1} & (ABC)_{n-1,n-1} \end{bmatrix}$$

where a is a scalar.

2.2 THE OPERATION OF TRANSPOSITION

Transposition means exchange of rows and columns of a matrix. We will denote this operation by T, and the transpose of a matrix A by A^T.

DEFINITION The *transpose* of a matrix $A = (a_{ij}) \in F_{m,n}$ is the matrix $A^T = (b_{ij}) \in F_{n,m}$ where $b_{ij} = a_{ji}$.

It can happen that $A^T = A$ for a square matrix $A = (a_{ij}) \in F_{n,n}$. Such a square matrix is called a *symmetric* matrix. A square matrix A such that $A^T = -A$ is called a *skew-symmetric* matrix.

Let

$$A = \begin{bmatrix} 1 & 2 & -3 \\ 4 & -5 & 7 \end{bmatrix} \qquad B = \begin{bmatrix} 5 & -4 & 1 \\ -4 & 6 & -4 \\ 1 & -4 & 5 \end{bmatrix}$$

$$C = \begin{bmatrix} 0 & 1 & 2 \\ -1 & 0 & -3 \\ -2 & 3 & 0 \end{bmatrix}$$

It is easy to verify that

$$A^T = \begin{bmatrix} 1 & 4 \\ 2 & -5 \\ -3 & 7 \end{bmatrix}$$

and the matrices B and C are symmetric and skewsymmetric, respectively.

DEFINITION The *trace* of a square matrix $A = (a_{ij}) \in F_{n \times n}$ is defined to be the sum of the elements on the main diagonal of A. The trace of A is designated as $tr(A)$, and we have

$$tr(A) = \sum_{i=1}^{n} a_{ii} \tag{2.2.1}$$

We shall list several important algebraic rules involving transposes and trace.

The Laws of the Transpose and the Trace

If $A = (a_{ij})$, $B = (b_{ij})$ are in $F_{m \times n}$, and $c \in F$, then

$$\begin{aligned} (A^T)^T &= A \\ (A + B)^T &= A^T + B^T \\ (cA)^T &= c(A^T) \end{aligned} \tag{2.2.2}$$

These laws of the transpose are easy to prove. We now give the following important theorem involving the transpose of the product of two matrices.

THEOREM 2.2 If $A = (a_{ij}) \in F_{m \times n}$ and $B = (b_{ij}) \in F_{n \times p}$, then $(AB)^T = B^T A^T$. In words, the transpose of the product AB is the product of their transposes in reverse order.

Proof. To prove the theorem, we compute the (i, j)-entry of each side of the equation $(AB)^T = B^T A^T$, as in the proof of Theorem 2.1. Thus

$$[(AB)^t]_{ij} = [AB]_{ji} = \sum_{k=1}^{n} a_{jk} b_{ki}.$$

Similarly,

$$[B^t A^t]_{ij} = [b_{1i}, b_{2i}, \ldots, b_{ni}] \begin{bmatrix} a_{j1} \\ a_{j2} \\ \vdots \\ a_{jn} \end{bmatrix} = \sum_{k=1}^{n} b_{ki} a_{jk} = \sum_{k=1}^{n} a_{jk} b_{ki}.$$

This shows that

$$[(AB)^t]_{ij} = [B^t A^t]_{ij} \qquad \text{for each } i = 1, \ldots, p, \text{ and } j = 1, \ldots, m$$

and consequently $(AB)^t = B^t A^t$ as desired.

The basic properties of the trace for $A = [a_{ij}]$, $B = [b_{ij}] \in F_{n,n}$ and $c \in F$ are

$$\begin{aligned} tr(A + B) &= tr(A) + tr(B) \\ tr(cA) &= c\, tr(A) \\ tr(AB) &= tr(BA) \end{aligned} \tag{2.2.3}$$

Note that the proofs of the first two are trivial. The third can be proved by direct computation of AB and BA and then summing up their diagonal entries.

Exercises 2.2

1. (Generalization of Theorem 2.2) If A_i, $i = 1, \ldots, m$, $m \geq 2$, are matrices for which the product $A_1 A_2 \cdots A_m$ is defined, show that

$$(A_1 A_2 \cdots A_m)^t = A_m^t A_{m-1}^t \cdots A_1^t$$

In words, the transpose of a product of m matrices is equal to the product of their transposes in reverse order.

2. Let $A, B \in F_{n,n}$. Show that $AB^t = BA^t$.
3. Let $A = (a_{ij})_{n,n}$. Prove that AA^t and $A^t A$ are always symmetric.
4. Show that any square matrix in $C_{n,n}$ can be written as a sum of two matrices, one symmetric and the other skewsymmetric.
5. Let $A \in R_{l,m}$, $B \in R_{m,n}$ and $C \in R_{n,l}$. Show that $(A\,B\,C)^t = C^t B^t A^t$.
6. Let A and B be symmetric matrices. Show that AB is also symmetric if and only if A and B commute.
7. If $A, B \in R_{n,n}$ prove that the relation $AB - BA = I$ cannot be valid. [Hint $tr(AB) = tr(BA)$.]